

Executive Order _____
National Security Information

It is vital that certain information in the Government's possession be uniformly protected against unauthorized disclosure. It also is essential that the public be informed concerning the activities of its Government. The interests of the United States and its citizens require that certain information concerning our national defense and foreign relations be given only limited dissemination. To ensure that such information is adequately safeguarded, this Order identifies the information to be so protected, prescribes classification, declassification, and safeguarding standards to be followed, and establishes a monitoring system to ensure its effectiveness.

SECTION 1. ORIGINAL CLASSIFICATION.

1-1. Classification Designation.

1-101. Information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified in one of the three categories listed below. Information and material shall be protected at an appropriate level of classification until a final determination is made as to the need for protection and the level of required protection. No other categories of classification shall be used to identify information or material as requiring protection in the interest of national security, except as otherwise provided

by statute. Nothing in this Order shall be construed as limiting the protection afforded national security information by other provisions of law.

1-102. "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

1-103. "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

1-104. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

1-2. Classification Authority.

1-201. Top Secret. Authority for original classification of information as Top Secret may be exercised only by the President, by such agency heads or officials as the President may designate by publication in the Federal Register, and by officials to whom such authority is delegated in accordance with Section 1-204.

1-202. Secret. Authority for original classification of information as Secret may be exercised only by such agency heads or officials as the President may designate by publication in the Federal Register, by officials who have Top Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204.

1-203. Confidential. Authority for original classification of information as Confidential may be exercised only by such agency heads or officials as the President may designate by publication in the Federal Register, by officials who have Top Secret or Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204.

1-204. Limitation on Delegation of Original Classification Authority.

(a) Authority to originally classify information as Top Secret may be delegated only to principle subordinate officials who have a need to exercise such authority as determined by the President, by agency heads designated pursuant to Section 1-201 or by senior officials designated in writing to exercise this authority by such agency heads.

(b) Authority to originally classify information as Secret may be delegated only to subordinate officials who have a need to exercise such authority as determined by the President, by agency heads designated pursuant to Section 1-201 and 1-202, and by officials with Top Secret classification authority.

(c) Authority to originally classify information as Confidential may be delegated only to subordinate officials who have a need to exercise such authority as determined by

Section 1-201, 1-202, and 1-203, and by officials with Top Secret classification authority.

(d) Delegated original classification authority may not be redelegated.

(e) Each delegation of original classification authority shall be in writing by name or title of position held.

(f) Delegations of original classification authority shall be limited to the absolute minimum required to exercise such authority to effectively and efficiently administer this Order. Agency heads shall implement procedures that ensure that officials so designated have a demonstrable and continuing need to exercise such authority.

1-205. Exceptional Cases. When an employee or contractor of an agency that does not have original classification authority originates information believed to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly under adequate safeguards to the agency which has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If

it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office for review. The Director shall consult with any agency determined to have a subject matter interest in this information before making any decision in this regard.

1-3. Classification Requirements.

1-301. Information may be considered for classification, and is thus classifiable, if it concerns:

- (a) military plans, weapons, or operations;
- (b) the vulnerabilities or capabilities of systems, installations, projects, or plans vital to the national security;
- (c) foreign government information;
- (d) intelligence activities, sources or methods;
- (e) foreign relations or foreign activities of the United States;
- (f) scientific, technological, or economic matters relating to the national security;

(g) United States Government programs for safeguarding nuclear materials or facilities;

(h) cryptology;

(i) an individual whose life or safety may be placed in jeopardy by disclosure of such information;

(j) techniques, procedures or material relating to the protective mission of the United States Secret Service; or

(k) other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by senior agency officials designated pursuant to Section 5-404(a).

1-302. Information which is determined to concern one or more of the criteria in Section 1-301 may be classified only when an original classification authority also determines that its unauthorized disclosure reasonably could be expected to cause damage to the national security. In considering whether the disclosure of information could be expected to cause damage to the national security, it is not necessary to consider such information in isolation. Information may be classified if its unauthorized disclosure, in conjunction with one or more other disclosures, reasonably could be expected to cause such damage.

1-303. Unauthorized disclosure of foreign government information, information which could compromise the identity of a confidential source, or information relating to intelligence sources, methods, and activities is presumed to cause damage to the national security. The classification status of the above described information shall not be affected by any unofficial publication in the United States or abroad of identical or similar information.

1-4. Duration of Classification.

1-401. Information shall be classified for as long as required by national security considerations. Guidelines shall be developed by agencies to ensure the effectiveness and integrity of the classification system while eliminating the accumulation of classified information which no longer requires protection. These guidelines shall facilitate the identification of information which should be considered for downgrading or declassification based on the degree to which the passage of time or the occurrence of a specific event or events may have eliminated or reduced the original national security sensitivity of this information. To the extent practicable, original classification authorities shall set a specific date or event for declassification at the time the information is originally classified.

1-5. Identification and Markings.

1-501. At the time of original classification, the following should be shown on the face of all classified documents, and prominently displayed, where practicable, on all other forms of classified information, except where such markings would reveal a confidential source or relationship not otherwise evident from the face of such documents or information:

- (a) the office of origin;
- (b) if appropriate, the date or event for declassification or review; and
- (c) one of the three classification designations defined in Section 1-1.

1-502. Only the designations Top Secret, Secret, or Confidential may be used to identify classified information. Markings such as "For Official Use Only" and "Limited Official Use" may not be used for that purpose. Terms such as "Sensitive" or "Agency" may not be used in conjunction with the classification designations prescribed by this Order; e.g., "Agency Confidential" or "Sensitive/Secret."

1-503. Each classified document, to the extent practicable, shall be marked or shall otherwise indicate which portions are classified with the appropriate classification designation, and

which portions are not classified. Agency heads designated pursuant to Section 1-2 may, for good cause, except specified classes of documents or information from this portion-marking requirement.

1-504. Foreign government information shall either retain its original classification designation or be assigned a United States classification designation that shall ensure a degree of protection equivalent to that required by the entity that furnished the information.

1-505. Classified documents that contain or reveal information that is subject to special dissemination and reproduction limitations authorized by this Order shall be marked clearly so as to place the user on notice of the restrictions.

1-6. Prohibitions.

1-601. Classification shall be determined solely on the basis of national security considerations. In no case shall information be classified in order to conceal violations of law, inefficiency or administrative error, to prevent embarrassment to a person, or organization or agency, or to restrain competition, or to prevent for any other reason the release of information which does not require protection in the interest of national security.

1-602. Classification may not be used to limit dissemination of information that is not classifiable under the provisions of this Order or to prevent or delay the public

1-603. A document may be classified after an agency has received a request for the document under the Freedom of Information Act or the Mandatory Review provisions of this Order (Section 3-4) if such classification is consistent with this Order and is authorized by the agency head, the deputy agency head, or by a senior agency official designated pursuant to Section 5-404. Classification authority under this provision shall be exercised personally, on a document-by-document basis.

1-604. Information which has been reviewed for declassification under the procedural and substantive criteria of E.O. 12065 pursuant to a Freedom of Information Act or Mandatory Review request which is still pending at the time this Order becomes effective, need not be rereviewed under the provisions of this Order.

SECTION 2. DERIVATIVE CLASSIFICATION.

2-1. Use of Derivative Classification.

2-101. Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide.

2-102. Persons who apply such derivative classification markings shall:

(a) observe and respect original classification decisions, which shall not be altered by the use of a classification level, time limit, or other marking different from the original on any copy, extract, paraphrase, restatement, or summary of any classified item except as specified under approved procedures for downgrading, declassification, or classification review in accordance with Section 3 below; and

(b) carry forward to any newly created documents any assigned dates or events for declassification or review and any additional authorized markings. A single marking may be used for documents based on multiple sources.

2-2. Classification Guides.

2-201. Agencies may promulgate classification guides to facilitate the proper and uniform classification of information. These guides may also be used to direct derivative classification. To the extent that information is classified pursuant to these guides, such classification is derivative classification and will be marked accordingly.

Section 3. DECLASSIFICATION AND DOWNGRADING.

3-1. Declassification Authority.

3-101. Information shall be declassified or downgraded as soon as national security considerations permit. Information that continues to meet the classification requirements prescribed by Section 1-3 despite the passage of time will continue to be protected in accordance with that section.

3-102. Agencies shall designate appropriate officials to exercise declassification and downgrading authority. To the fullest extent practicable, such authority will be exercised by the official who authorized the original classification if that official is still serving in the same position, or by the originator's officially authorized successor.

3-103. The provisions of this section relating to declassification shall apply to agencies which, under the terms of this Order, do not have authority to originally classify information, but which had such authority under prior orders.

3-2. Transferred Information.

3-201. In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.

3-202. In the case of classified information which is not officially transferred in accordance with Section 3-201, but originated in an agency which has ceased to exist, each agency in possession shall be deemed to be the originating agency for

purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consulting with any other agency which has an interest in the subject matter of the information.

3-203. Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded or declassified in accordance with this Order, with directives of the President issued through the National Security Council, and with agency guidelines promulgated in consultation with the Information Security Oversight Office.

3-3. Systematic Review for Declassification.

3-301. Agency heads designated pursuant to Section 1-2 and the heads of agencies which had original classification authority under prior orders may establish procedures for the systematic review of classified information for the purpose of declassifying or downgrading such information in accordance with the classification requirements of Section 1-3. Guidelines concerning systematic review for declassification may be issued by such agency heads for classified information under their jurisdiction after consultation with the Archivist of the United States and review by the Information Security Oversight Office. Information for which no systematic declassification guidelines are issued, or information which is not identified in these guidelines as requiring systematic review, and for which a prior automatic declassification date has not been established, will be

subject Approved For Release 2005/08/02 : CIA-RDP85-00988R000200240011-3 Both the mandatory review for declassification provisions of Section 3-4.

3-302. The Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence sources and methods. These guidelines, if developed, will be used by the Archivist of the United States or any agency having custody of this information.

3-4. Mandatory Review for Declassification.

3-401. All classified information and material shall be subject to a classification review by the originating agency at any time after the expiration of ten years from the date of the information's origin provided:

(1) A United States person or United States federal, state, or local governmental body or agency requests a review;

(2) The request describes the record with sufficient specificity to enable the agency to locate it; and

(3) The record can be located and obtained with a reasonable amount of effort.

3-402. This procedure shall apply to information classified under this Order or prior orders. Requests for declassification under this provision shall be acted upon within 60 days. After review, information that no longer requires protection under this Order shall be declassified and released unless withholding is otherwise warranted under applicable law.

3-403. Requests for mandatory review shall be processed in accordance with procedures developed by agency heads in consultation with the Archivist of the United States and the Information Security Oversight Office. These procedures shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information.

3-404. Special procedures for the review of classified cryptologic information shall be established by the Secretary of Defense, and by the Director of Central Intelligence for information pertaining to intelligence sources and methods. These procedures shall be implemented only after appropriate consultation with affected agencies. Agencies having custody of classified cryptologic or intelligence source or method information will process requests for mandatory review of such information in accordance with these procedures. Disputes concerning the implementation of these procedures, or the procedures developed pursuant to Section 3-403, may be appealed to the National Security Council.

3-405. Requests for declassification of classified

documents originated by an agency but in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 note, shall be referred by the Archivist to the agency of origin for processing in accordance with the above provisions and for direct response to the requestor. The Archivist shall inform requestors of such referrals, unless this notification would confirm the existence or nonexistence of the requested documents, which fact is itself classifiable under the Order. In such cases, the Archivist will respond to the requestor in accordance with Section 3-406 below.

3-406. An agency may, in response to a request for records under the Freedom of Information Act or this Order's Mandatory Review provision, refuse to confirm or deny the existence or non-existence of the information or material, when the fact of its existence or non-existence would itself be classifiable under the Order.

3-407. Requests for declassification which are submitted under the provisions of the Freedom of Information Act shall be processed in accordance with the provisions of that Act.

SECTION 4. SAFEGUARDING.

4-1. General Restrictions on Access.

4-101. A person is eligible for access to classified information only after a favorable determination of trustworthiness has been reached by agency heads or designated senior officials based upon appropriate investigations in

accordance with applicable standards and criteria, and provided that such access is essential to the accomplishment of official Government duties or contractual obligations. Agency heads listed in section 1-2 shall issue and maintain minimum security investigative standards that must be satisfied for each of the three national security information classification designations before access to such information is provided.

4-102. Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons. Originating agencies may place restrictions on the reproduction of classified documents and establish other accountability controls in conformity with this policy of protecting classified information from unauthorized disclosure.

4-103. Classified information disseminated outside the Executive Branch shall be given protection equivalent to that afforded within the Executive Branch.

4-104. Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency.

4-2. Special Access Programs.

4-201. Agency heads designated pursuant to Section 1-201 may create special access programs to control access,

distribution, and protection of particularly sensitive information classified pursuant to this Order or prior orders. Procedures governing the creation, continuance, and maintenance of such special access programs will be developed by the above agency heads. For special access programs pertaining to intelligence sources and methods, this function will be exercised by the Director of Central Intelligence, who will ensure the implementation of common security, access, dissemination and control standards for such programs.

4-3. Access by Historical Researchers and Former Presidential Appointees.

4-301. The requirement in Section 4-101 that access to classified information may be granted only as is necessary for the performance of official duties may be waived as provided in Section 4-302 for persons who:

- (a) are engaged in historical research projects, or
- (b) previously have occupied policy-making positions to which they were appointed by the President.

4-302. Waivers under Section 4-301 may be granted only if the agency with jurisdiction over the information:

- (a) makes a written determination that access is consistent with the interests of national security; and

(b) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that such information is safeguarded in a manner consistent with this Order.

SECTION 5. IMPLEMENTATION AND REVIEW.

5-1. Oversight.

5-101. The National Security Council may review all matters with respect to the implementation of this Order and shall provide overall policy direction for the information security program. The National Security Council will be assisted in this monitoring function by the Information Security Oversight Office.

5-2. Information Security Oversight Office.

5-201. The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Administrator also shall have authority to appoint a staff for the Office.

5-202. The Director shall:

(a) oversee agency actions to ensure compliance with this Order and implementing directives;

(b) consider and take action on complaints and suggestions from persons within or outside the Government

Approved For Release 2005/08/02 : CIA-RDP85-00988R000200240011-3
with respect to the administration of the information
security program;

(c) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order;

(d) report annually to the President through the Administrator of General Services and the National Security Council on the implementation of this Order;

(e) review any agency implementing regulations promulgated pursuant to Section 3-301 (systematic declassification) or 3-403 (mandatory declassification requests);

(f) review requests for original classification authority from agencies or officials not granted original classification authority pursuant to Section 1-2; and

(g) have authority to require each agency to furnish such reports or information, consistent with the protective purposes of this Order, as is necessary to fulfill his responsibilities.

5-3. Interagency Information Security Committee.

5-301. There is established an Interagency Information Security Committee which shall be comprised of representatives of the Secretaries of State, Defense, Treasury, and Energy, the Attorney General, the Director of Central Intelligence, the National Security Council, the Domestic Policy Staff, the Archivist of the United States, the Information Security Oversight Office, and a Chairman designated by the President.

5-302. Representatives of other agencies may be invited to meet with the Committee on matters of particular interest to those agencies.

5-303. The Committee shall meet at the call of the Chairman or at the request of a member agency and shall advise the Chairman on implementation of this Order.

5-4. General Responsibilities.

5-401. Agencies which originate or handle classified information shall:

(a) designate a senior agency official to conduct an active oversight program to ensure effective implementation of this Order. This program shall familiarize agency and other personnel who have access to classified information with the provisions of this Order and implementing directives and shall impress upon agency personnel their responsibility to exercise vigilance in complying with this Order;

(b) establish a process to decide appeals from denials of declassification requests submitted pursuant to Section 3-4; and

(c) establish procedures to prevent unnecessary access to classified information, including procedures which require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and which ensures that the number of persons granted access to classified information is reduced to and maintained at the minimum number that is consistent with operational and security requirements and needs.

5-402. Unclassified implementing directives or regulations promulgated pursuant to this Order will be published in the FEDERAL REGISTER.

5-5. Sanctions.

5-501. If the Information Security Oversight Office finds that a violation of this Order or any implementing directive may have occurred, it shall make a report to the head of the agency concerned so that corrective steps may be taken.

5-502. Officers and employees of the United States Government shall be subject to appropriate sanctions if they:

(a) knowingly, willfully and without authorization disclose information or materials properly classified under this Order or prior orders or compromise properly classified information through negligence; or

(b) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or

(c) knowingly, willfully or negligently violate any other provision of this Order or implementing directive.

Unauthorized disclosure for purposes of this section includes either a communication or physical transfer of classified information or materials to an unauthorized person.

5-503. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and agency regulations.

5-504. Agency heads shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5-502 occurs. The Director of the Information Security Oversight Office shall be informed when such violations occur.

5-505. Agency heads shall report to the Attorney General evidence reflected in classified information of possible

violations of Federal criminal law by an agency employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General.

SECTION 6. GENERAL PROVISIONS.

6-1. Definitions.

6-101. "Agency" has the meaning provided at 5 U.S.C. 552(e).

6-102. "Classified information" means information or material, herein collectively termed information, that is owned by, produced for or by, or under the control of, the United States Government, and that has been determined pursuant to this Order or prior orders to require protection against unauthorized disclosure, and that is so designated.

6-103. Foreign government information means:

(a) Documents, material, or information provided by a foreign government or governments, an international organization of governments, or any element thereof in the expectation, expressed or implied, that this document, material, or information is to be held in confidence; or

(b) Classified information or material produced by the United States pursuant to or as a result of a joint

Approved For Release 2005/08/02 : CIA-RDP85-00988R000200240011-3
arrangement, with a foreign government or organization of
governments requiring that the information, the arrangement,
or both be held in confidence.

6-104. "National security" means the national defense and
foreign relations of the United States.

6-105. "Confidential source" means the identity of any
individual or organization which has provided, or which may
reasonably be expected to provide, information to the United
States with the expectation, expressed or implied, that the
information or relationship or both be held in confidence.

6-2. General.

6-201. Nothing in this Order shall supersede any
requirement made by or under the Atomic Energy Act of 1954, as
amended. "Restricted Data" and information designated as
"Formerly Restricted Data" shall be handled, protected,
classified, downgraded, and declassified in conformity with the
provisions of the Atomic Energy Act of 1954, as amended, and
regulations issued pursuant thereto.

6-202. The Attorney General, upon request by the head of an
agency, his duly designated representative, or the Director of
the Information Security Oversight Office, shall personally or
through authorized representatives of the Department of Justice
render an interpretation of this Order with respect to any
question arising in the course of its administration.

6-203. Executive Order No. 12065 of June 28, 1978, is revoked as of the effective date of this Order.

6-204. This Order shall become effective on _____, 1981.